

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION**

DEBBIE HALE and NICK MARGEAS,
individually and on behalf of all others
similarly situated,

Plaintiffs,

v.

AT&T Inc.,

Defendant.

Case No. 3:24-cv-1943

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiffs Debbie Hale and Nick Margeas (“Plaintiffs”), individually and on behalf of all others similarly situated and defined as:

All persons (i) with the wireless carriers T-Mobile, Verizon, Black Wireless, Boost Infinite, Consumer Cellular, Cricket Wireless, FreedomPop, FreeUp Mobile, Good2Go, H2O Wireless, PureTalk, Red Pocket, Straight Talk Wireless, TracFone Wireless, Unreal Mobile, Wingor, and any other mobile virtual network operators (MVNOs) that used AT&T’s network for the period May 1, 2022 to October 31, 2022 or for the period January 2023, and (ii) whose personally identifiable information was accessed and/or acquired in the data incident that is the subject of the Data Breach announced by AT&T on July 12, 2024

(“the Class” and “Class Members”), upon personal knowledge of the facts pertaining to themselves and upon information and belief as to all other matters, by and through their counsel, hereby bring this Class Action Complaint against Defendant AT&T Inc. (“AT&T” or “Defendant”). The Class alleged in this Complaint specifically excludes persons whose wireless carrier was AT&T between May 1, 2022 and October 31, 2022 and January 2023.

INTRODUCTION

1. On or about July 12, 2024, Defendant AT&T admitted that information about more than 100 million of its customers' cellular telephone calls and texts were exposed in a massive data breach perpetrated by cybercriminals (the "New Data Breach") in or about April of 2024.

2. AT&T also disclosed that the compromised data included the telephone numbers and text records of the Class members, i.e. customers of wireless providers that used its network between May 1, 2022 and October 31, 2022, as well as a number of Class members that used its network in January 2023, and the records of their telephone numbers and texts.

3. The stolen logs contain a record of virtually every number Class members called or texted - including customers of other wireless networks - the number of times they interacted and the call duration.

4. The foregoing data is personally identifiable information ("PII") and is valuable and sensitive.

5. Plaintiffs learned of the New Data Breach on or after July 12, 2024.

6. Plaintiffs bring this Class Action on behalf of themselves and all non-AT&T customers harmed by AT&T's misconduct.

JURISDICTION AND VENUE

7. Jurisdiction is proper in this Court under 28 U.S.C § 1332 (diversity jurisdiction). This Court has subject matter and diversity jurisdiction over this case pursuant to 28 U.S.C. § 1332(d) because: (1) this is a class action where the amount in controversy in this class action exceeds five million dollars (\$5,000,000), excluding interest and costs; (2) there are more than 100 Class members; (3) at least one member of the Class is diverse from the Defendant; and (4) the Defendant is not a government entity.

8. Supplemental jurisdiction to adjudicate issues pertaining to state law is proper in this Court under 28 U.S.C. § 1367.

9. Defendant is headquartered and has its principal place of business in the Dallas Division of the Northern District of Texas and has sufficient minimum contacts with and intentionally avails itself of the markets in this State.

10. Venue is proper in this District under 28 U.S.C. § 1391 because a substantial part of the events that gave rise to Plaintiff's claims occurred within the Dallas Division of the Northern District of Texas, where AT&T is headquartered.

PARTIES

11. Plaintiff Debbie Hale is a resident of Dallas County, Iowa and citizen of the United States. For the period May 1, 2022 to October 31, 2022 and January 2023, Plaintiff's wireless carrier was Verizon.

12. Plaintiff Nick Margeas is a resident of Polk County, Iowa and citizen of the United States. For the period May 1, 2022 to October 31, 2022 and January 2023, Plaintiff's wireless carrier was T-Mobile.

13. Defendant AT&T is a corporation organized under the laws of Delaware with its principal place of business located at 208 South Akard Street, Dallas, Texas 75202.

FACTUAL ALLEGATIONS

A. On July 12, 2024, AT&T Announced a New Data Breach.

14. On July 12, 2024, AT&T announced that "customer data was illegally downloaded from [it's] workspace on a third-party cloud platform. We launched an investigation and engaged cybersecurity experts to understand the nature and scope of the criminal activity. We have taken steps to close off the illegal access point."

15. On the same day, AT&T posted a notice of “Unlawful Access of Customer Data” notice on its website.¹ AT&T provided several suggestions to affected customers as to how to protect themselves from “phishing, smishing, and other online fraud.”

16. AT&T also apologized to its customers for the New Data Breach and admitted that it has an obligation to protect the information in its care. *Id.*

B. AT&T’s Announcement ignored the impact on Class members, who are not AT&T customers.

17. AT&T’s announcement did not disclose that Class members’ data was also illegally downloaded during the New Data Breach.

18. Some Class members have contracts with mobile virtual network operators (“MVNOs”). A mobile virtual network operator (“MVNO”) is a wireless communications services provider that does not own the wireless network infrastructure over which it provides services to its customers. An MVNO enters into a business agreement with a mobile network operator, here AT&T, to obtain bulk access to network services at wholesale rates, then sets retail prices independently.

19. On information and belief, the MVNOs which contracted with AT&T to use AT&T’s network services during the relevant time periods include, but may not be limited to, Black Wireless, Boost Infinite, Consumer Cellular, Cricket Wireless, FreedomPop, FreeUp Mobile, Good2Go, H2O Wireless, PureTalk, Red Pocket, Straight Talk Wireless, TracFone Wireless, Unreal Mobile, and Wingor.

20. Because MVNOs use AT&T’s network, the Class members’ data was accessed during the New Data Breach just as if they were customers of AT&T. However, AT&T has not taken steps to warn the Class members of the New Data Breach or its impact on them.

¹<https://www.att.com/support/article/my-account/000102979> (last accessed July 25, 2024).

21. Further, on information and belief, T-Mobile and Verizon have agreements with AT&T or its subsidiaries that permit roaming on their networks to customers of each of the companies.²

22. For example, AT&T, T-Mobile, and Verizon customers are able to place calls just as they normally would, but their calls are carried by whichever network is most operational in their area.

23. Accordingly, AT&T maintains data of telephone calls and text records made by T-Mobile or Verizon customers but which were carried on AT&T's network.

24. Because T-Mobile and Verizon use AT&T's network, the Class members' data was accessed during the New Data Breach just as if they were customers of AT&T. However, AT&T has not taken steps to warn the Class members of the New Data Breach or its impact on them.

C. AT&T has not been transparent about its security failures with its own customers much less with Class Members.

25. AT&T has not been transparent about the nature and extent of data security lapses impacting its customers – and thus by extension, has not been transparent with Class members.

26. This is the second massive data breach that AT&T has announced in 2024. In or about March 2024, Defendant AT&T admitted that it lost control over its current and former customers' highly sensitive personal information in a data breach perpetrated by cybercriminals (the "March 2024 Data Breach").

27. The March 2024 Data Breach exposed the personal information of an estimated total of 73 million customers. Upon information and belief, this information includes full names, email addresses, mailing phone numbers, dates of birth, and Social Security numbers, as well as

²<https://www.t-mobile.com/news/press/att-and-t-mobile-open-networks-to-customers-of-both-carriers-in>

AT&T account numbers and AT&T encrypted passcodes that can be used to access AT&T customer accounts.

28. In addition to the massive March 2024 Data Breach, several years prior to that a cybercriminal indicated that he had taken millions of AT&T customers' data. AT&T did not sufficiently warn its customers that they were in danger of identity theft and worse until years later. For years, bad actors had access to information enabling them to impersonate, defraud, and spy on AT&T's unsuspecting customers.

29. Notwithstanding its history of massive data breaches, AT&T has not done enough to protect its affected customers, much less to protect Class members from which it is profiting by carrying the Class members' calls and texts.

30. AT&T failed to adequately safeguard Class members' PII allowing cybercriminals to access this wealth of priceless information/or years before AT&T warned its customers to be on the lookout.

31. AT&T had an obligation created by reasonable industry standards, common law, and representations to Class members and the Class members' carriers to keep their PII confidential and to protect the information from unauthorized access.

32. The PII of Plaintiffs and Class Members was shared with AT&T with the reasonable expectations and mutual understanding that AT&T would comply with its obligations to keep such information confidential and secure from unauthorized access.

33. Because the Data Breach was an intentional hack by cybercriminals seeking information of value that they could exploit, victims are at imminent risk of severe identity theft and exploitation.

34. Plaintiffs have suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from AT&T's failures to safeguard their PII being placed in the hands of unauthorized third parties, including strangers and possibly criminals.

35. Plaintiffs have a continuing interest in ensuring that their PII, which, upon information and belief, remains backed up in AT&T's possession, is protected and safeguarded from future breaches and leaks.

36. AT&T owed a duty to Plaintiffs and the Class members whose PII was entrusted to AT&T to disclose in a timely and accurate manner when data breaches occurred.

37. AT&T owed a duty of care to Plaintiffs and the Class members because they were foreseeable and probable victims of any inadequate data security practices.

38. AT&T knew or should have known that AT&T's computer and/or electronic systems were targets for theft and other cybersecurity attacks because the warning signs were readily available and accessible via the Internet.

39. This Data Breach has and will lead to fulfil their devastating financial and personal losses to Class members. As a direct and proximate result of the Data Breach, Plaintiffs and the Class members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud, blackmail, and identity theft. Plaintiffs and the Class members will now have to spend time and money to mitigate the actual and potential impact of the Data Breach on their everyday lives, including but not limited to placing "freezes" with the credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and reviewing and addressing unauthorized activity for years to come.

40. Plaintiffs and Class members have suffered, and continue to suffer, actual harms for which they are entitled to compensation, including:

- a. Trespass, damage to and theft of their personal property, including PII;
- b. Improper disclosure of their PII;
- c. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals and having been already misused;
- d. Damages flowing from AT&T's failure to notify Class members (who are non-AT&T customers) of the Data Breach;
- e. Loss of privacy suffered as a result of the Data Breach; and
- f. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the Data Breach.

D. Plaintiffs' Experience

41. During the relevant period, Plaintiff Debbie Hale was a wireless customer of Verizon. On information and belief, as a customer of Verizon, Plaintiff Hale's PII was shared with AT&T in connection with roaming or shared services provided by AT&T. Further, Plaintiff Hale communicated via text and phone call with at least two AT&T wireless customers during the relevant period. Accordingly, on information and belief, Plaintiff Hale's PII was subject to the Data Breach.

42. Plaintiff Hale typically takes measures to protect their PII and is very careful about sharing their PII. For example, Plaintiff stores any documents containing their PII in a safe and secure location. She diligently chooses unique usernames and passwords for their telecommunications accounts.

43. During the relevant period, Plaintiff Nick Margeas was a wireless customer of T-Mobile. On information and belief, as a customer of T-Mobile, Plaintiff Margeas' PII was shared with AT&T in connection with roaming or shared services provided by AT&T. Further, Plaintiff Margeas communicated via text and phone call with at least two AT&T wireless customers during the relevant period. Accordingly, on information and belief, Plaintiff Margeas' PII was subject to the Data Breach.

44. Plaintiff Margeas typically takes measures to protect their PII and is very careful about sharing their PII. For example, Plaintiff stores any documents containing their PII in a safe and secure location. He diligently chooses unique usernames and passwords for their telecommunications accounts.

45. As a result of the Data Breach, Plaintiffs now face the possibility that malevolent actors will blackmail them with the information disclosed in this Data Breach and therefore have sustained emotional distress.

46. Plaintiffs also suffered actual injury in the form of damages to and diminution in the value of their PII – a form of intangible property that was entrusted to AT&T for the purpose of obtaining services from AT&T or communicating with AT&T customers, which was compromised in and as a result of the Data Breach.

47. Plaintiffs face imminent and impending injury arising from the disclosure of sensitive personal information that has already occurred as well as the substantially increased.

48. As a result of the Data Breach, Plaintiffs are at a substantial additional present risk and will continue to be at an increased risk of blackmail, identity theft, and fraud for years to come.

49. To date, AT&T has failed to notify Class members that their PII was affected by the Data Breach even though they are not customers of AT&T, has failed to adequately protect

Plaintiffs and Class Members, and has failed to compensate them for their injuries sustained in this Data Breach.

CLASS ACTION ALLEGATIONS

50. Pursuant to the provisions of Federal Rules of Civil Procedure 23(a), 23(b)(1), 23(b)(2), 23(b)(3), and 23(c)(4), Plaintiffs seek to bring this class action on behalf of themselves and a nationwide class (the “Nationwide Class”), defined as follows:

All persons (i) with the wireless carriers T-Mobile, Verizon, Black Wireless, Boost Infinite, Consumer Cellular, Cricket Wireless, FreedomPop, FreeUp Mobile, Good2Go, H2O Wireless, PureTalk, Red Pocket, Straight Talk Wireless, TracFone Wireless, Unreal Mobile, Wingor, and any other mobile virtual network operators (MVNOs) that used AT&T’s network³ for the period May 1, 2022 to October 31, 2022 or the period of January 2023, and (ii) whose personally identifiable information was accessed and/or acquired in the data incident that is the subject of the Data Breach announced by AT&T on July 12, 2024.

51. Excluded from the Class are AT&T; officers, directors, and employees of AT&T; any entity in which AT&T has a controlling interest, is a parent or subsidiary, or which is controlled by AT&T; and the affiliates, legal representatives, attorneys, heirs, predecessors, successors, and assigns of AT&T. Also excluded are Plaintiffs’ attorneys, including all attorneys and other employees of their law firms. Also excluded are the Judges and Court personnel in this case and any members of their immediate families.

52. Plaintiffs reserve the right to modify and/or amend the Nationwide Class, including, but not limited to, creating additional subclasses, as necessary.

³ Plaintiffs reserve the right to amend the Class definition based on discovery.

53. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of the claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

54. All Class Members are readily ascertainable in that their respective wireless carriers have access to addresses and other contact information for all Class Members, which can be used for providing notice to Class Members.

55. **Numerosity.** Consistent with Rule 23(a)(1) of the Federal Rules of Civil Procedure, the Nationwide Class is so numerous that joinder of all members is impracticable. While the exact number of Nationwide Class Members is unknown, upon information and belief, it is in the millions and is certain to be in excess of 100 individuals.

56. **Commonality and Predominance.** Consistent with Federal Rules of Civil Procedure 23(a)(2) and (b)(3), this action involves common questions of law and fact that predominate over any questions that may affect only individual Class Members. Such common questions include:

- a. whether AT&T engaged in the wrongful conduct alleged in this Complaint;
- b. whether AT&T's conduct was unfair, unconscionable, and/or unlawful;
- c. whether AT&T failed to implement and maintain adequate and reasonable systems and security procedures and practices to protect Plaintiffs and Class Members' PII;
- d. whether AT&T owed a duty to Plaintiffs and Class Members to adequately protect their PII and to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;
- e. whether AT&T breached its duties to protect the PII of Plaintiffs and Class Members by failing to provide adequate data security and failing to provide appropriate and adequate notice of the Data Breach to Plaintiffs and Class Member;
- f. whether AT&T's conduct was negligent;
- g. whether AT&T knew or should have known that its systems were vulnerable to being compromised;

- h. whether AT&T's conduct, including its failure to act, resulted in or was the proximate cause of the Data Breach of its systems, resulting in the loss of Plaintiffs and Class Members' PII;
- i. whether AT&T wrongfully or unlawfully failed to inform Plaintiffs and Class Members that it did not maintain data security practices adequate to reasonably safeguard Plaintiffs and Class Members' PII;
- j. whether Plaintiffs and Class Members suffered injury, including ascertainable losses, as a result of AT&T's conduct (or failure to act);
- k. whether Plaintiffs and Class Members are entitled to recover damages; and
- l. whether Plaintiffs and Class Members are entitled to declaratory relief and equitable relief, including injunctive relief, restitution, disgorgement, and/or other equitable relief.

57. **Typicality.** Consistent with Federal Rule of Civil Procedure 23(a)(3), Plaintiffs claims are typical of the claims of other Class Members in that Plaintiffs, like all Class Members, had their personal data compromised, breached, and stolen in the Data Breach. Plaintiffs and all Class Members were injured through the misconduct of AT&T and assert the same claims for relief.

58. **Adequacy.** Consistent with Federal Rule of Civil Procedure 23(a)(4), Plaintiffs and their counsel will fairly and adequately protect the interests of the Class. Plaintiffs are members of the Class they seek to represent; are committed to pursuing this matter against AT&T to obtain relief for the Class; and have no interests that are antagonistic to, or in conflict with, the interests of other Class Members. Plaintiffs retained counsel who are competent and experienced in litigating class actions and complex litigation, including privacy litigation of this kind. Plaintiffs and their counsel intend to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

59. **Superiority.** Consistent with Federal Rule of Civil Procedure 23(b)(3), a class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual

actions or piecemeal litigation. Moreover, absent a class action, most Class Members would find the cost of litigating their claims prohibitively high and would therefore have no effective remedy, so that in the absence of class treatment, AT&T's violations of law inflicting substantial damages in the aggregate would go unremedied without certification of the Class. Plaintiffs and Class Members have been harmed by AT&T's wrongful conduct and/or action. Litigating this action as a class action will reduce the possibility of repetitious litigation relating to AT&T's conduct and/or inaction. Plaintiffs know of no difficulties that would be encountered in this litigation that would preclude its maintenance as a class action.

60. Class certification, therefore, is appropriate under Federal Rule of Civil Procedure 23(b)(3) because the common questions of law or fact predominate over any questions affecting individual Class Members, a class action is superior to other available methods for the fair and efficient adjudication of this controversy, and the requirements of Rule 23(a) are met.

61. Class certification is also appropriate under Federal Rule of Civil Procedure 23(b)(2), in that the prosecution of separate actions by the individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for AT&T. In contrast, the conduct of this action as a class action conserves judicial resources and the parties' resources and protects the rights of each Class Member. Specifically, injunctive relief could be entered in multiple cases, but the ordered relief may vary, causing AT&T to have to choose between differing means of upgrading its data security infrastructure and choosing the court order with which to comply. Class action status is also warranted because prosecution of separate actions by Class Members would create the risk of adjudications with respect to individual Class Members that, as a practical matter, would

be dispositive of the interests of other members not parties to this action, or that would substantially impair or impede their ability to protect their interests.

62. Class certification is also appropriate under Federal Rule of Civil Procedure 23(b)(2) because AT&T, through its uniform conduct, acted or failed and refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole. Moreover, AT&T continues to maintain its inadequate security practices, retain possession of Plaintiffs and Class Members' PII, and has not been forced to change its practices or to relinquish PII by nature of other civil suits or government enforcement actions, thus making injunctive relief a live issue and appropriate to the Class as a whole.

63. Particular issues are also appropriate for certification under Federal Rule of Civil Procedure 23(c)(4) because the claims present particular, common issues, the resolution of which would materially advance the resolution of this matter and the parties' interests therein.

COUNT I

Negligence (On Behalf of Plaintiffs and the Nationwide Class)

64. Plaintiffs repeat and re-allege and incorporate by reference herein all of the allegations contained in the foregoing paragraphs.

65. Plaintiffs bring this claim on behalf of themselves and the Nationwide Class.

66. AT&T offered and provided the wireless carriers of Plaintiffs and Class Members services that inevitably involved the submission of sensitive personal information from Plaintiffs and Class members, including the phone numbers they called and texted, which is their sensitive and non-public PII. AT&T collected, stored, used, and benefited from this non-public PII of Plaintiffs and Class Members in the provision of providing telecommunications services to Plaintiffs and Class Members (and their respective wireless carriers).

67. Plaintiffs and Class Members entrusted AT&T with their PII and AT&T was fully cognizant of the value and importance of the PII and the types of harm that Plaintiffs and Class Members could and would suffer if the PII were wrongfully disclosed.

68. AT&T negligently created a dangerous situation by failing to take adequate and reasonable steps to safeguard Plaintiffs and Class Members' sensitive PII from unauthorized release or theft.

69. AT&T owed an independent duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, securing, deleting, protecting, and safeguarding the sensitive PII, and preventing the PII from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

70. AT&T was required to prevent foreseeable harm to Plaintiffs and Class Members. Accordingly, AT&T had a duty to take adequate and reasonable steps to safeguard their sensitive PII from unauthorized release or theft. AT&T's duties, included, but were not limited to: (1) designing, maintaining, and testing its data security systems, data storage architecture, and data security protocols to ensure Plaintiffs and Class Members' PII in its possession was adequately secured and protected; (2) implementing processes that would detect an unauthorized breach of its security systems and data storage architecture in a timely and adequate manner; (3) timely acting on all warnings and alerts, including public information, regarding its security vulnerabilities and potential compromise of the PII of Plaintiffs and Class Members; and (4) maintaining data security measures consistent with industry standards and applicable federal and state laws and other requirements.

71. AT&T owed a common law duty to prevent foreseeable harm to Plaintiffs and Class Members. The duty existed because Plaintiffs and Class Members were the foreseeable and

probable victims of any inadequate security practices of AT&T in its collection, storage, and use of PII from Plaintiffs and Class Members. It was foreseeable that Plaintiffs and Class Members would be harmed by the failure to protect their PII because malicious actors routinely attempt to steal such information for use in nefarious purposes, such as blackmail, fraud, identity theft, and other forms of impersonation.

72. AT&T's obligation to use adequate and reasonable security measures also arose because AT&T collected, stored, and used the PII of Plaintiffs and Class Members for the procurement and provision of telecommunications services per its agreement with Class members' wireless carriers.

73. Additionally, the policy of preventing future harm weighs in favor of finding AT&T owed a duty to Plaintiffs and Class Members.

74. AT&T also owed a duty to timely disclose the material fact that its computer systems and data security practices and protocols were inadequate to safeguard users' personal calling and text-messaging data from theft and other misuses, including without limitation blackmail, fraud, identity theft, and other forms of impersonation.

75. The injuries suffered by Plaintiffs and Class Members were proximately and directly caused by AT&T's failure to follow reasonable, industry standard security measures to protect Plaintiffs' and Class Members' PII.

76. When individuals have their personal information stolen, they are at substantial risk for imminent identity theft, and need to take additional steps to protect themselves following this unprecedented Data Breach.

77. If AT&T had implemented the requisite, industry-standard security measures and exercised adequate and reasonable care, data thieves would not have been able to take the PII of Plaintiffs and Class Members.

78. AT&T breached these duties through the conduct alleged here in this Complaint by, including without limitation, failing to protect the PII in its possession; failing to maintain adequate computer systems and allowing unauthorized access to and exfiltration of Plaintiffs and Class Members' PII; failing to disclose the material fact that AT&T's computer systems and data security practices were inadequate to safeguard the PII in its possession from theft; and failing to disclose in a timely and accurate manner to Plaintiffs and Class Members the material facts of the Data Breach.

79. But for AT&T's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, their PII would not have been compromised. And, as a direct and proximate result of AT&T's failure to exercise adequate and reasonable care and use commercially adequate and reasonable security measures, the PII of Plaintiffs and Class Members was accessed by ill-intentioned individuals who could and will use the information to commit identity or financial fraud. Plaintiffs and Class Members face the imminent, certainly impending, and substantially heightened risk of identity theft, fraud, and further misuse of their personal data.

80. There is a temporal and close causal connection between AT&T's failure to implement security measures to protect the PII collected from Class Members and the harm suffered, or risk of imminent harm suffered, by Plaintiffs and Class Members.

81. It was foreseeable that AT&T's failure to exercise reasonable care to safeguard the PII in its possession or control would lead to one or more types of injury to Plaintiffs and Class

Members. The Data Breach was also foreseeable given the known, high frequency of cyberattacks and data breaches in the telecommunications industry.

82. Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. AT&T knew of or should have known of the inherent risks in collecting and storing PII, the critical importance of providing adequate security of PII, the current cyber scams being perpetrated on PII, and that it had inadequate protocols, including security protocols in place to secure the PII of Plaintiffs and Class Members.

83. AT&T's own conduct created the foreseeable risk of harm to Plaintiffs and Class Members. AT&T's misconduct included its failure to take the steps and opportunities to prevent the Data Breach and its failure to comply with industry standards for the safekeeping, encryption, and authorized disclosure of the PII of Plaintiffs and Class Members.

84. Plaintiffs and Class Members have no ability to protect their PII that was and is in AT&T's possession. AT&T alone was, and is, in a position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Data Breach.

85. As a direct and proximate result of AT&T's negligence as alleged above, Plaintiffs and Class Members have suffered, will suffer, or are at increased risk of suffering:

- a. The compromise, publication, theft and/or unauthorized use of their PII;
- b. Unauthorized use and misuse of their PII;
- c. The loss of the opportunity to control how their PII are used;
- d. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from blackmail, fraud, identity theft, and other forms of impersonation;
- e. Lost opportunity costs and lost wages and time associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from blackmail, fraud, identity theft, and other forms of impersonation;

f. The imminent and certain impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals;

g. The continued risk to their PII that is subject to further breaches so long as AT&T fails to undertake appropriate measures to protect the PII in AT&T's possession; and

h. Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate, and repair the impact of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

86. Pursuant to the FTC Act, 15 U.S.C. § 45, AT&T had a duty to provide fair and adequate computer systems and data security measures to safeguard the PII of Plaintiffs and Class Members.

87. The FTC Act prohibits "unfair ... practices in or affecting commerce," 15 U.S.C. § 45(a)(1), which the FTC has interpreted to include businesses' failure to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of AT&T's duty in this regard. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

88. AT&T solicited, gathered, and stored PII of Plaintiffs and Class Members to facilitate transactions that affect commerce.

89. AT&T's violation of the FTC Act (and similar state statutes) constitutes negligence.

90. Plaintiffs and Class Members are within the class of persons that the FTC Act (and similar state statutes) were intended to protect.

91. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act (and similar state statutes) seeks to prevent. The FTC has pursued enforcement actions against businesses which, as a result of their failure to employ adequate and reasonable data security measures, caused the same harm as that suffered by Plaintiffs and Class Members.

92. As a direct and proximate result of AT&T's violations of the above-mentioned statutes (and similar state statutes), Plaintiffs and Class Members have suffered, and continue to suffer, damages arising from the Data Breach as described herein and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

RELIEF REQUESTED

WHEREFORE, Plaintiffs, individually and on behalf of the proposed Nationwide Class, request the following relief:

- a. An order certifying this case as a class action on behalf of the Nationwide Class, defined above, appointing Plaintiffs as Class representative thereof and appointing the undersigned counsel as Class counsel thereof;
- b. An order directing notice to the Class of the effects of the Data Breach on their PII;
- c. A mandatory injunction directing AT&T to adequately safeguard Plaintiffs and the Class's PII by implementing improved security procedures and measures as outlined above;
- d. An award of other declaratory, injunctive, and equitable relief as is necessary to protect the interests of Plaintiffs and Class Members;
- e. An award of restitution and compensatory, consequential, and general damages to Plaintiffs and Class Members, including nominal damages as allowed by law in an amount to be determined at trial or by this Court;
- f. An award of actual or statutory damages to Plaintiffs and Class Members in an amount to be determined at trial or by this Court;
- g. An award of reasonable litigation expenses and costs and attorneys' fees

to the extent allowed by law;

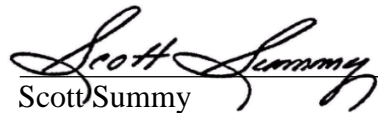
- h. An award to Plaintiffs and Class Members of pre- and post-judgment interest, to the extent allowable; and
- i. Award of such other and further relief as equity and justice may require.

E. JURY TRIAL DEMANDED

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiffs demand a trial by jury of any and all issues in this action so triable as of right.

Dated: July 30, 2024

Respectfully submitted,



Scott Summy
Texas Bar No. 19507500
BARON & BUDD, P.C.
3102 Oak Lawn Ave # 1100
Dallas, TX 75219
Phone: (214) 521-3605
Fax: (214) 523-6600
ssummy@baronbudd.com

Elizabeth A. Fegan
Megan Shannon
FEGAN SCOTT LLC
150 S. Wacker Dr., 24th Floor
Chicago, IL 60606
Phone: (630) 273-2625
Fax: (312) 264-0100
beth@feganscott.com
megan@feganscott.com

J. Barton Goplerud
Shindler, Anderson, Goplerud &
Weese P.C.
5015 Grand Ridge Dr., Ste. 100
West Des Moines, IA 50265
Phone: (515) 223-4567
goplerud@sagwlaw.com